CHICAGO POLICE DEPARTMENT
DEPLOYMENT OPERATIONS CENTER

CRIME PREVENTION AND INFORMATION CENTER (CPIC) PRIVACY POLICY

Chicago Police Department's Crime Prevention Information Center

Privacy, Civil Rights, and Civil Liberties Protection Policy

A. Purpose Statement

1. The purpose of the Privacy, Civil Rights, and Civil Liberties Protection Policy (hereafter "Privacy Policy") is to promote **the Chicago Police Department's Crime Prevention Information Center** (hereafter "C.P.I.C."), source agency, and user agency (hereafter collectively referred to as "participating agencies" or "participants") conduct that complies with applicable federal, state, local, and tribal laws, regulations, and policies (see Appendix A – Terms and Definitions, of this policy) and assists participants in:
   - Ensuring individual privacy, civil rights, civil liberties, and other protected interests.
   - Increasing public safety and improving national security.
   - Protecting the integrity of criminal investigatory, criminal intelligence, and justice systems processes and information.
   - Minimizing the threat and risk of injury to specific individuals and damage to real or personal property.
   - Minimizing reluctance of individuals or groups to use or cooperate with the justice systems.
   - Encouraging individuals or community groups to trust and cooperate with the justice system.
   - Promoting governmental legitimacy and accountability.
   - Making the most effective use of public resources allocated to public safety agencies.

B. Policy Applicability and Legal Compliance

1. All participating CPIC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, and other authorized users will comply with the CPIC's privacy policy. This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including Information sharing Environment (ISE) participating centers and agencies), and participating justice and public safety agencies, as well as private contractors, private entities, and the general public.

2. The CPIC will provide a printed copy of its Privacy Policy to all CPIC personnel, non-agency personnel who provide services to the CPIC, and to each source agency and CPIC authorized user and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

3. All CPIC personnel, participating agency personnel, personnel providing information technology services to the CPIC, private contractors, and other authorized users shall comply with applicable laws protecting privacy, civil rights, civil liberties, and other

protected interests, including, but not limited to, the U.S. Constitution, the Illinois Constitution, 28 Code of Federal Regulations (CFR) Part 23, Illinois Freedom of Information Act (5 ILCS 140/1, et seq.) and all other state, local, and federal privacy, civil rights, civil liberties, and legal requirements (refer to Appendix B) applicable to the CPIC and/or other participating agencies.

4. The CPIC has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to, those listed in Appendix B.

C. Governance and Oversight

1. The Commander of the CPIC will have primary responsibility for operating the CPIC, system operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and enforcing the provisions of this policy.

2. A privacy committee of designees as determined by the Superintendent of Police will ensure that privacy and civil rights are protected as provided in this policy and by the Chicago Police Department's information-gathering and collection, retention, and dissemination processes and procedures. The committee will annually review and recommend updates to the policy to the Commander of the CPIC in response to changes in law, including the results of audits and inspections.

3. The CPIC's privacy committee is guided by a trained Privacy Officer who is selected by the CPIC Commander to assist in enforcing the provisions of this policy and who, in addition to other responsibilities, will receive reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the CPIC's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented throughout the process. The CPIC Privacy Officer can be reached at the below listed mailing or email address:

   Chicago Police Department – CPIC
   c/o Privacy Officer
   3510 S. Michigan, 4th Floor
   Chicago, IL 60653
   cpicpo@chicagopolice.org

4. The CPIC Privacy Officer ensures that enforcement procedures and sanctions outlined in this policy are adequate and enforced.

D. Terms and Definitions

1. The primary terms and definitions used in this privacy policy are set forth in Appendix A, Terms and Definitions.

E. Information

1. The CPIC will seek or retain information which a source agency (the CPIC or other agency) has determined that:
   - Is based on possible threat to public safety or the enforcement of criminal law, or
   - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents, the resulting justice system response, or the prevention of crime, or
   - Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
   - Is useful in crime analysis or in the administration of criminal justice and public safety, and
   - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
   - The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

   The CPIC may retain information that is based on a level of suspicion that is less that "reasonable suspicion", such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified within this policy.

2. Source agencies will agree not to submit information, and the CPIC will not seek or retain information about any individual or organization that was gathered solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientation.

3. The CPIC applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

   - The information is protected information as defined by the center to include personal information on any individual (see center's definitions of "protected information" and "personal information" in Appendix A of policy), and, to the extent expressly provided in this policy, to include organizational entities.
   - The information is subject to Illinois and federal law (Appendix B) restricting access, use, or disclosure.

4. The CPIC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as:
   - Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
   - The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
   - The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
   - The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

5. At the time a decision is made by the CPIC to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

   - Protect confidential sources and police undercover techniques and methods.
   - Not interfere with or compromise pending criminal investigations.
   - Protect an individual's right of privacy or their civil rights and civil liberties.
   - Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

6. The labels assigned to existing information under Section E. 5. will be reevaluated whenever:

   - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
   - There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

7. CPIC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. Center personnel will:

   - Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format and data collection codes for SAR information.

- Store the information using the same storage method used for data that rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).
- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Retain SAR information for one (1) year to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

8. The CPIC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

9. The CPIC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the Information Sharing Environment. Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

10. The CPIC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:
    - The name of the originating center, department or agency, component, and subcomponent.
    - The name of the center's justice information system from which the information is disseminated.
    - The date the information was collected and, where feasible, the date its accuracy was last verified.

- The title and contact information for the person to whom questions regarding the information should be directed.

11. The CPIC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

12. The CPIC will keep a record of the source of all information sought and collected by the center.

F. Acquiring and Receiving Information

1. Information-gathering (acquisition) and access and investigative techniques used by the CPIC and source agencies must comply with and adhere to applicable laws, regulations and guidelines, including, but not limited to:
    - U.S. and Illinois state constitutional provisions (including those listed in Appendix B).
    - Applicable federal and state law provisions.
    - Chicago ordinances and regulations.
    - 28 CFR Part 23 regarding criminal intelligence information.
    - The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy).
    - Criminal Intelligence guidelines established under the U.S. Department of Justice's National Criminal Intelligence Sharing Plan (NCISP).

2. The CPIC's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and other personnel at source agencies who acquire SAR information that may be shared with the CPIC will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

3. The CPIC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

4. Information-gathering and investigative techniques used by the CPIC, and those used by originating agencies, should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

5. External agencies that access the CPIC's information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

6. The CPIC will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.

7. The CPIC will not directly or indirectly receive, seek, accept, or retain information from:
    - An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.
    - An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

G. Information Quality Assurance

1. The CPIC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

2. The CPIC will ensure that source agencies assume primary responsibility for the quality and accuracy of their information collected by the CPIC. The CPIC will advise the appropriate contact person in the source agency in writing (this would include electronic notification) if information received from the source agency is alleged, suspected, or found to be erroneous or deficient.

3. The CPIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other related information about the same individual or organization only when the applicable standard (refer to Section I, Merging Records) has been met.

4. At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]).

5. The labeling of retained information will be reevaluated by the CPIC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

6. The CPIC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the center did not have authority to gather the information or to provide the information to another agency; or the center used prohibited means to gather the information (except when the center's information source did not act as the agent of the center in gathering the information).

7. Originating agencies external to the CPIC are responsible for reviewing the quality and accuracy of the data provided to the center. The center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

8. The CPIC will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

H. Collation and Analysis

1. Information acquired or received by the CPIC or accessed for other sources will be analyzed only by qualified CPIC personnel who have successfully completed a background check and any applicable security clearance and have been selected, approved, and trained accordingly.

2. Information subject to collation and analysis is Information as defined and identified in Section E, Information of this policy.

3. Information acquired or received by the CPIC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:
   - Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the CPIC.
   - Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.

The CPIC requires that all analytical products be reviewed by the Privacy Officer, or qualified designee as determined by the Commander of CPIC, to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

I. Merging Records

1. The set of identifying information sufficient to allow merging by the CPIC will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

2. If the matching requirements are not fully met but there is an identified partial match, the information may be associated by the CPIC if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

J. Sharing and Disclosure

1. Credentialed, role-based access criteria will be used by the CPIC, as appropriate, to control:
    A. The information to which a particular group or class of users can have access based on the group or class
    B. The information a class of users can add, change, delete, or print.
    C. To whom, individually, the information can be disclosed and under what circumstances

2. The CPIC adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

3. Access to or disclosure of records retained by the CPIC will be provided only to persons within the center or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information accessed will be kept by the CPIC.

4. Agencies external to the CPIC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

5. Records retained by the CPIC may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

6. Information gathered or collected and records retained by the CPIC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of four (4) years by the CPIC.

7. Information gathered or collected and records retained by the CPIC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the center for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

8. Information gathered or collected and records retained by the CPIC will not be:
   - Sold, published, exchanged, or disclosed for commercial purposes.
   - Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
   - Disseminated to persons not authorized to access or use the information.

9. There are several categories of records that will not be ordinarily not be provided to the public:
   - Pursuant to Illinois Freedom of Information Act, 5 ILCS 140 *et al.,* the following records will not be provided to the public:
     1. Information specifically prohibited from disclosure by federal or state law or rules and regulations implementing federal or state law.
     2. Private information, unless disclosure is required by another provision of this Act, a state or Federal law or courts order.
     3. Personnel information contained within public records, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy,

unless disclosure is consented to in writing by the individual subjects of the information.

4. Records that relate to or affect the security of correctional institutions and detention facilities.
5. Preliminary drafts, notes, recommendations, memorandum and other records in which opinions are expressed, or policies or actions are formulated, except that a specific record or relevant portion of the record shall not be exempt when the record is publicly cited and identified by the head of the public body.
6. Trade secrets and commercial or financial information from a person or business where trade secrets or commercial or financial information are furnished under a claim of proprietary, privileged or confidential, and that disclosure would cause competitive harm to the person or business, and only insofar as the claim directly applies to the records requested.
7. Records relating to collective negotiating matters between public bodies and their employees or representatives, except that any final contract or agreement shall be subject to inspection and copying.
8. Records relating to a public body's adjudication of employee grievances or disciplinary cases; however, this exemption does not extend to the final outcome of cases in which discipline is imposed.
9. Information that would disclose or might lead to the disclosure of secret or confidential information, codes algorithms, programs, or private keys intended to be used to create electronic or digital signatures under the Electronic Commerce Security Act.
10. Vulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community, but not to the extent that disclosure could reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public. Information exempt under this item may include such things as details pertaining to the mobilization or deployment of personnel or equipment, to the operation of communication systems or protocols, or to tactical operations.
11. Records in the possession of any body created in the course of administrative enforcement proceedings, and any law enforcement or correctional agency for law enforcement purposes, but only to the extent that disclosure would:
    1. interfere with pending or actually and reasonably contemplated law enforcement proceedings conducted by any law enforcement or correctional agency that is the recipient of the request;
    2. interfere with active administrative enforcement proceedings conducted by the public body that is the recipient of the request;
    3. create a substantial likelihood that a person will be deprived of a fair trial or an impartial hearing;

4. unavoidably disclose the identity of a confidential source, confidential information furnished only by the confidential source, or persons who file complaints with or provide information to administrative, investigative, law enforcement, or penal agencies; except that the identities of witnesses to traffic accidents, traffic accident reports, and rescue reports shall be provided by agencies of local government, except when disclosure would interfere with an active criminal investigation conducted by the agency that is the recipient of the request;
5. disclose unique or specialized investigative techniques other than those generally used and known or disclose internal documents or correctional agencies related to detection, observation or investigation of incidents of crime or misconduct, and disclosure would result in demonstrable harm to the agency or public body that is the recipient of the request;
6. endanger the life or physical safety of law enforcement personnel or any other person; or
7. obstruct an ongoing criminal investigation by the agency that is the recipient of the request.

- Information that meets the definition of "classified information" as the term is defined in the National Security Act, Public Law 235, Section 606, and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
- Information determined to be confidential under Section 4002 of the Technology Advancement and Development Act.
- Information contained in local emergency plan submitted to a municipality in accordance with a local emergency plan ordinance that is adopted under Section 11-21.5-5 of the Illinois Municipal Code.
- Law enforcement officer identification information or driver information under Section 11-212 of the Illinois Vehicle Code.
- Information prohibited from being disclosed by the Personnel Records Review Act.
- Information prohibited from being disclosed by the Illinois School Student Records Act.
- Information that would violate an authorized nondisclosure agreement.
- Information of personally identifiable health information pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and any other confidentiality law.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission.
- Other authorized basis for denial.

10. The CPIC will not confirm the existence or nonexistence of information to any person, or agency that would not be entitled to receive the information unless otherwise required by law.

K. Redress

K.1 Disclosure:

1. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in item 2, below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the CPIC. The individual may obtain a copy, if appropriate or required, of the information for the purpose of challenging the accuracy or completeness of the information. The CPIC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual. In Illinois, an individual's right to access and review criminal history record information is codified under Title 20, Part 1210 of the Illinois Administrative Code.

2. The existence, content, and source of the information will not be made available to an individual when:
   - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (5ILCS 140/7(1)(d)(i)).
   - Disclosure would endanger the health or safety of an individual, organization, or community (5ILCS 140/7(1)(d)(vi)).
   - The information is in a criminal intelligence information system subject to 28 CFR Part 23.
   - Other authorized basis for denial (refer to Section J, Sharing and Disclosure).

   If the information does not originate with the CPIC, the requestor will be referred to the originating agency, if appropriate or required, or the CPIC will notify the source agency of the request and its determination that disclosure by the CPIC or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

K.2 Corrections

If an individual requests correction of information originating with the CPIC that has been disclosed, the CPIC's Privacy Officer or designee will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.

K.3 Appeals

The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for correction(s) are denied by the CPIC or the originating agency. The individual will also be informed of the procedure for appeal when the CPIC or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

K.4 Complaints

1. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:

   A. Is exempt from disclosure,

   B. Has been or may be shared through the ISE,

      i) Is held by the CPIC and

      ii) Allegedly has resulted in demonstrable harm to the complainant,

   The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the CPIC's Privacy Officer at the following e-mail address: cpicpo@chicagopolice.org or at that mailing address as found in Section N.1(2) of this policy. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the CPIC that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the CPIC Privacy Officer of all complaints and the resulting action taken in response to the complaint.

2. To delineate protected information shared through the ISE from other data, the CPIC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

L. Security Safeguards

1. The CPIC's Senior Watch Officer (SWO) is designated and trained to serve as the CPIC's security officer.

2. The CPIC will operate in a secure facility that is protected from external intrusion. The CPIC will utilize secure internal and external safeguards against network intrusions. Access to the CPIC's databases from outside the facility will be allowed only over secure networks.

3. The CPIC will secure tips, leads and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

4. The CPIC will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by CPIC personnel authorized to take such actions.

5. Access to CPIC's information will be granted only to CPIC personnel whose positions and job duties require such access; who have successfully completed a background check and applicable security clearance; and who have been selected, approved, and trained accordingly.

6. Queries made to the CPIC's data applications will be logged into the data system identifying the user initiating the query.

7. The CPIC will utilize logs to maintain audit trails of requested and disseminated information (see Section N.2, Accountability, for more information on audit logs).

8. The CPIC will follow the data breach notification guidance set forth in the Illinois Personal Information Protection Act, 815 ILCS 530. The CPIC will:
    i. Notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person.
    ii. Make any necessary notice promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the breach or any measures necessary to determine the scope of the breach and, if necessary, to restore the integrity of any information system affected by this release.

9. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

M. Information Retention and Destruction

1. The CPIC's Privacy Officer will ensure that all information is reviewed for record retention (validation or purge) at least every two (2) years and in accordance with the Department's Form Retention Schedule and as provided by 28 CFR Part 23. For purposes of this Privacy Policy and for records retention and destruction purposes, suspicious activity reports will be treated as Chicago Police Department Information Reports which have a twelve (12) month retention.

2. When information has no further value or meets the CPIC's criteria for removal according to the Chicago Police Department's retention and destruction policy or according to the Illinois State Records Act, it will be purged, destroyed, and deleted or returned to the submitting agency.

3. The CPIC will delete information or return it to the originating agency once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency.

4. The CPIC's Privacy Officer will complete a Department To-From Subject report through the chain of command accompanied by a Record Destruction Report per Department policies and procedures and in accordance with the Department's Form Retention Schedule for notification of appropriate parties before information is deleted or returned in accordance with this policy or as otherwise agreed upon with the originating agency.

5. Notification of proposed destruction or return of records may or may not be provided to the submitting agency by the CPIC depending on the relevance of the information and any agreement with the originating agency.

6. A record of information to be reviewed for retention will be maintained by the CPIC, and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

N. Transparency, Accountability, and Enforcement

N.1 Information System Transparency

1. The CPIC will be open with the public in regard to information and intelligence collection policies and practices. The CPIC will make the CPIC's Privacy Policy available upon request and posted on the Center's Web page at www.chicagopolice.org.

2. The CPIC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The CPIC Privacy Officer can be contacted at:

Chicago Police Department
c/o CPIC Privacy Officer
3510 S. Michigan, 4th Floor

Chicago, IL 60653
cpicpo@chicagopolice.org

N.2 Accountability

1. The audit log of queries made to the CPIC will identify the user initiating the query.

2. The CPIC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of four (4) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

3. The CPIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least semiannually and a record of the audits will be maintained by the CPIC Privacy Officer of the center.

4. CPIC's personnel or other authorized users shall report errors or suspected or confirmed violations of the CPIC's policies relating to protected information to the CPIC's Privacy Officer.

5. The CPIC will conduct an annual audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted by CPIC's Privacy Officer, or a designee as determined by the Superintendent of Police for the Chicago police Department. This person has the option of conducting a random audit at any time and without prior notice to the CPIC staff. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the CPIC's information and intelligence system(s).

6. The Department's Office of Compliance and/or CPIC's trained Privacy Officer will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will make appropriate changes in response to changes in applicable laws, technology, the purpose and use of the information systems and public expectations.

N.3 Enforcement

1. If center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Director of the CPIC will:
   - Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.

- Suspend, demote, transfer, or terminate center personnel, as permitted by applicable Department personnel policies.
- Apply administrative actions or sanctions as provided by Department General Order 93-03 entitled "Complaint and Disciplinary Procedures" and all addendum of General Order 93-03 in conjunction with the Rules and Regulations of the Chicago Police Department.
- If the authorized user is from an agency external to the agency/center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The CPIC reserves the right to restrict the qualifications and number of personnel having access to CPIC information and to suspend or withhold service and deny access to participating agency or participating agency personnel violating the CPIC's Privacy Policy.

O. Training

1. The CPIC will require the following individuals to participate in training programs regarding implementation of and adherence to this privacy, civil rights, and civil liberties policy:
   - All assigned personnel of the CPIC.
   - Personnel providing information technology services to the CPIC.
   - Staff in other public agencies or private contractors providing services to the CPIC.
   - User who are not employed by the CPIC or a contractor.

2. The CPIC's privacy policy training program will cover:

   - Purposes of the privacy, civil rights, and civil liberties protection policy.
   - Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained or submitted by the CPIC to the shared space.
   - Originating and participating agency responsibilities and obligations under applicable law and policy.
   - Department guidelines and procedures regarding the First Amendment and Police Actions, Modified Consent Decree regarding First Amendment investigations (Alliance to End Repression v. City of Chicago, 237 F.3d 799(7^{th} Cir. 2001)), Judgment Order concerning First Amendment Rights and a hostile audience (Nelson v. Streeter, No. 88 C 5434), and Judgment Order concerning Attorney-Client Relationships (Case 76 C 1982).
   - How to implement the policy in the day-to-day work of the user, whether a paper or system user.
   - The impact of improper activities associated with infractions within or through the agency.

- Mechanisms for reporting violations of the CPIC's privacy protection policies and procedures.
- The nature and possible penalties for policy violations, including possible transfer, dismissal, and criminal liability, and immunity, if any.

3. The CPIC will provide special training regarding the center's requirements and policies for collection, use and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

Appendix A—Terms and Definitions

The following is a list of primary terms and definitions used throughout this policy. These terms may also be useful in drafting the definitions section of the agency's/center's privacy policy.

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Access Control—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Acquisition—The means by which an ISE participant obtains information through the exercise of its authorities, for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer either to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

Agency—The **CPIC** and all agencies that access, contribute, and share information in the **CPIC**'s justice information system.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—Authentication is the process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

Authorization—The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

Biometrics—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Center—Center refers to the Chicago Police Department's **Crime Prevention & Information Center or CPIC.**

Civil Liberties—Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Civil Rights—The term "civil rights" refers to governments' role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

Computer Security—Protection of information assets through the use of technology, processes, and training.

Confidentiality—Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

Credentials—Information that includes identification and proof of identification that is utilized by CPIC members to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates. Credentialed security access will be utilized to control:

- What information a class of users can have access to;
- What information a class of users can add, change, delete, or print; and
- To whom the information can be disclosed and under what circumstances.

Criminal Intelligence Information or Data—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information. The record is maintained per 28 CFR Part 23.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disk optical media.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and faxback systems. It does not include faxes, telephone calls, video

Fair Information Practices—The Fair Information Practices (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transporter Flows of Personal Data. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system. They are designed to:

1. Define agency purposes for information to help ensure agency uses of information are appropriate. ("Purpose Specification Principle")

2. Limit the collection of personal information to that required for the purposes intended. ("Collection Limitation Principle")

3. Ensure data accuracy. ("Data Quality Principle")

4. Ensure appropriate limits on agency use of personal information. ("Use Limitation Principle")

5. Maintain effective security over personal information. ("Security Safeguards Principle")

6. Promote a general policy of openness about agency practices and policies regarding personal information. ("Openness Principle")

7. Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency. ("Individual Participation Principle")

8. Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies. ("Accountability Principle")

Firewall—a security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

Fusion Center—A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

General Information or Data—Information that could include records, documents, or files pertaining to law enforcement operations, such as Computer Aided Dispatch (CAD) data, incident data, and management information. Information that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information could be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Homeland Security Information—As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

Information—Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, tips and leads data, suspicious activity reports, and criminal intelligence information.

Information Quality—Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy,

completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—A SAR that has been determined, pursuant to a two-part process established in the ISE SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Intelligence-Led Policing (ILP)—A process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

Invasion of Privacy—Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

Law—As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information—For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Logs—Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals can access the system and the data.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases) and non-electronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Metadata—In its simplest form, metadata is information (data) about information, more specifically information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

Need to Know— As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

Nonrepudiation—A technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

Originating Agency—The agency or organizational entity that documents information or data, including source agencies that document SAR (and, when authorized, ISE-SAR) information that is collected by a fusion center.

Participating Agencies—An organization entity that is authorized to access or receive and use center information and/or intelligence databases and resources for lawful purposes through its authorized individual users.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in an activity or incident potentially related to terrorism.

Personally Identifiable Information—Personally identifiable information is one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious

affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).

- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).

- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).

- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons—Executive Order 12333 defines "United States persons" as a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the right to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy—A printed, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, disclosure, and access. The purpose of the privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and -implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection—A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Private Information – Pursuant to Illinois Freedom of Information Act, 5 ILCS 140 *et al.*, Private Information means unique identifiers, including a person's social security number, driver's license number, employee identification number, biometric identifiers, personal financial information, passwords or other access codes, medical records, home or personal telephone

numbers, and personal email addresses. Private information also includes home address and personal license plates, except as otherwise provided by law or when compiled without possibility of attribution to any person.

Protected Information—Protected information includes personal data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Illinois constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and local laws and ordinances. Protection may also be extended to organizations by center policy or state or local law

For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.

Public—Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the agency's/center's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

- Employees of the agency.
- People or entities—private or governmental—who assist the agency/center in the operation of the justice information system.
- Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

Public Access—Public access relates to what information can be seen by the public, that is, information whose availability is not subject to privacy interests or rights.

Record—Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Redress—internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

Repudiation—the ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Retention—Refer to Storage.

Right to Know—Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

Role-Based Access—A type of access that uses roles to determine rights and privileges. A role is a symbolic category of users that share the same security privilege.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Source Agency—Source agency refers to the agency or entity that originates SAR (and, when authorized, ISE-SAR) information.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the Information Technology industry than the second meaning.
2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Suspicious Activity—Observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Reports (SARs)—Reports that record the observation and documentation of a suspicious activity. Suspicious Activity Report (SAR) information offers a standardized means for feeding information repositories or data analysis tool. Any patterns identified during SAR review and analysis may be investigated in coordination with the reporting agency and, if applicable, the state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

Terrorism Information—Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism-Related Information—In accordance with the IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in the IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)) and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside the agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview reports (FIR). However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have an criminal offense attached or indicated, criminal history records, or Computer Aided Dispatch (CAD) data. Tips and leads information

should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on whether time and resources are available to determine its meaning.

Tips and leads information is maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

User—An individual representing a participating agency who is authorized to access or receive and use a center's information and intelligence databases and resources for lawful purposes.

Appendix B –State and Federal Law Relevant to Seeking, Retaining, and Disseminating Justice Information

STATE LAW:

Constitution of the State of Illinois

Illinois Administrative Code, Title 20, **Corrections, Criminal Justice, and Law Enforcement**

Illinois Administrative Code, Title 20, Part 1210 **Individual's Right To Access and Review Criminal History Record Information**

Illinois Compiled Statutes (ILCS):

- **Civil Administrative Code of Illinois** (Department of State Police Law), Title 20, Part 2605/2605-45(4)
- **Illinois Freedom of Information Act**, 5 ILCS 140/1, et seq.
- **Illinois School Student Records Act**, Title 105, Part, Section 5
- **Illinois State Records Act**, 5 ILCS 160
- Municipalities, Title 65 Illinois Municipal Code, Part 5, Article 11, Division 21.5-5, **"Local Emergency Plans"**
- Personal Information Protection Act, Title 815, Part 530 and 815-530-10 **"Notice of Breach"**
- **Personnel Records Review Act**, Title 820, Part 40
- **Technology Advancement and Development Act**, Title 20, Part 700, Section 4002
- Vehicles, Title 65, Part 5, Chapter 11 **Illinois Vehicle Code**, 212 (law enforcement officer identification information or driver information)

FEDERAL LAW:

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data-Protecting Personal Privacy," December 20, 2000

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22

Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter I, Part 23

Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter I, Part 20

Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510 2522, 2701 2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510 2522, 2701 2709, and 3121 3125, Public Law 99-508

Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681

Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301

Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552

HIPAA, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191

HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164; Code of Federal Regulations, Title 45, Parts 160 and 164

Indian Civil Rights Act of 1968, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 1016, as amended by the 9/11 Commission Act

National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490

National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616

Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a

Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313

Protection of Human Subjects, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter I, Volume 2, Part 46

Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314

Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201

U.S. Constitution, First, Fourth, and Sixth Amendments

USA PATRIOT Act, Public Law 107-56 (October 26, 2001), 115 Stat.

Rahm Emanuel
Mayor

Department of Police – City of Chicago
3510 S. Michigan Avenue – Chicago, Illinois 60653

Garry F. McCarthy
Superintendent

Privacy Policy Agreement

I hereby agree that I have received a copy of the Crime Prevention and Information Center (hereinafter described as "CPIC") Privacy Policy and have read it and fully understand the CPIC Privacy Policy and the Privacy Principles contained therein. Additionally, I agree to abide by the Privacy Design Principles and guidelines contained within the CPIC Privacy Policy. Documents and information obtained in the CPIC may contain confidential or privileged information, by signing this agreement I agree to treat all communication obtained in the CPIC as Law Enforcement Sensitive for Official Use Only. I understand that any further distribution of these documents is restricted to law enforcement agencies unless otherwise approved by the Chicago Police Department. I understand and comply with the terms of the Privacy Policy Agreement and will adhere to the terms regarding distribution of information.

Member's Name _____

Member's Employee Number _____

Member's Signature _____

Date _____

Chicago Police Department's Crime Prevention Information Center

Privacy, Civil Rights, and Civil Liberties Protection Policy

A. Purpose Statement

1. The purpose of the Privacy, Civil Rights, and Civil Liberties Protection Policy (hereafter "Privacy Policy") is to promote **the Chicago Police Department's Crime Prevention Information Center** (hereafter "C.P.I.C."), source agency, and user agency (hereafter collectively referred to as "participating agencies" or "participants") conduct that complies with applicable federal, state, local, and tribal laws, regulations, and policies (see Appendix A – Terms and Definitions, of this policy) and assists participants in:
   - Ensuring individual privacy, civil rights, civil liberties, and other protected interests.
   - Increasing public safety and improving national security.
   - Protecting the integrity of criminal investigatory, criminal intelligence, and justice systems processes and information.
   - Minimizing the threat and risk of injury to specific individuals and damage to real or personal property.
   - Minimizing reluctance of individuals or groups to use or cooperate with the justice systems.
   - Encouraging individuals or community groups to trust and cooperate with the justice system.
   - Promoting governmental legitimacy and accountability.
   - Making the most effective use of public resources allocated to public safety agencies.

B. Policy Applicability and Legal Compliance

1. All participating CPIC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, and other authorized users will comply with the CPIC's privacy policy. This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies(including Information sharing Environment (ISE) participating centers and agencies), and participating justice and public safety agencies, as well as private contractors, private entities, and the general public.

2. The CPIC will provide a printed copy of its Privacy Policy to all CPIC personnel, non-agency personnel who provide services to the CPIC, and to each source agency and CPIC authorized user and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

3. All CPIC personnel, participating agency personnel, personnel providing information technology services to the CPIC, private contractors, and other authorized users shall comply with applicable laws protecting privacy, civil rights, civil liberties, and other

protected interests, including, but not limited to, the U.S. Constitution, the Illinois Constitution, 28 Code of Federal Regulations (CFR) Part 23, Illinois Freedom of Information Act (5 ILCS 140/1, et seq.) and all other state, local, and federal privacy, civil rights, civil liberties, and legal requirements applicable to the CPIC and/or other participating agencies.

4. The CPIC has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties.

C. Governance and Oversight

1. The Commander of the CPIC will have primary responsibility for operating the CPIC, system operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and enforcing the provisions of this policy.

2. A designee as determined by the Superintendent of Police will ensure that privacy and civil rights are protected as provided in this policy and by the Chicago Police Department's information-gathering and collection, retention, and dissemination processes and procedures. The above designee will periodically review and update the policy in response to changes in law, including the results of audits and inspections.

3. The CPIC is guided by a trained Privacy Officer who is selected by the CPIC Commander to assist in enforcing the provisions of this policy and who, in addition to other responsibilities, will receive reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the CPIC's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented throughout the process. The CPIC Privacy Officer can be reached at the below listed mailing or email address:

   Chicago Police Department – CPIC
   c/o Privacy Officer
   3510 S. Michigan, 4th Floor
   Chicago, IL 60653
   cpicpo@chicagopolice.org

4. The CPIC Privacy Officer ensures that enforcement procedures and sanctions outlined in this policy are adequate and enforced.

D. Terms and Definitions

1. The primary terms and definitions used in this privacy policy are set forth in Appendix A, Terms and Definitions.

E. Information

1. The CPIC will seek or retain information which a source agency (the CPIC or other agency) has determined that:
   - Is based on possible threat to public safety or the enforcement of criminal law, or
   - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents, the resulting justice system response, or the prevention of crime, or
   - Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
   - Is useful in crime analysis or in the administration of criminal justice and public safety, and
   - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
   - The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

   The CPIC may retain information that is based on a level of suspicion that is less that "reasonable suspicion", such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified within this policy.

2. Source agencies will agree not to submit information, and the CPIC will not seek or retain information about any individual or organization that was gathered solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientation.

3. The CPIC applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

   - The information is protected information as defined by the center to include personal information on any individual (see center's definitions of "protected information" and "personal information" in Appendix A of policy), and, to the extent expressly provided in this policy, to include organizational entities.
   - The information is subject to Illinois and federal law restricting access, use, or disclosure.

4. The CPIC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as:

- Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
- The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

5. At the time a decision is made by the CPIC to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

   - Protect confidential sources and police undercover techniques and methods.
   - Not interfere with or compromise pending criminal investigations.
   - Protect an individual's right of privacy or their civil rights and civil liberties.
   - Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

6. The labels assigned to existing information under this Section will be reevaluated whenever:

   - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
   - There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

7. CPIC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. Center personnel will:

   - Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format and data collection codes for SAR information.
   - Store the information using the same storage method used for data that rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.

- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).
- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Retain SAR information for one (1) year to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

8. The CPIC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

9. The CPIC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the Information Sharing Environment. Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

10. The CPIC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:
    - The name of the originating center, department or agency, component, and subcomponent.
    - The name of the center's justice information system from which the information is disseminated.
    - The date the information was collected and, where feasible, the date its accuracy was last verified.
    - The title and contact information for the person to whom questions regarding the information should be directed.

11. The CPIC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

12. The CPIC will keep a record of the source of all information sought and collected by the center.

F. Acquiring and Receiving Information

1. Information-gathering (acquisition) and access and investigative techniques used by the CPIC and source agencies must comply with and adhere to applicable laws, regulations and guidelines, including, but not limited to:
    - U.S. and Illinois state constitutional provisions
    - Applicable federal and state law provisions
    - Chicago ordinances and regulations
    - 28 CFR Part 23 regarding criminal intelligence information
    - The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy).
    - Criminal Intelligence guidelines established under the U.S. Department of Justice's National Criminal Intelligence Sharing Plan (NCISP)

2. The CPIC's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and other personnel at source agencies who acquire SAR information that may be shared with the CPIC will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

3. The CPIC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

4. Information-gathering and investigative techniques used by the CPIC, and those used by originating agencies, should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

5. External agencies that access the CPIC's information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

6. The CPIC will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.

7. The CPIC will not directly or indirectly receive, seek, accept, or retain information from:
    - An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.
    - An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

G. Information Quality Assurance

1. The CPIC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

2. The CPIC will ensure that source agencies assume primary responsibility for the quality and accuracy of their information collected by the CPIC. The CPIC will advise the appropriate contact person in the source agency in writing (this would include electronic notification) if information received from the source agency is alleged, suspected, or found to be erroneous or deficient.

3. The CPIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other related information about the same individual or organization only when the applicable standard (refer to Section I, Merging Records) has been met.

4. At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]).

5. The labeling of retained information will be reevaluated by the CPIC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

6. The CPIC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the center did not have authority to gather the information or to provide the information to another agency; or the center used

prohibited means to gather the information (except when the center's information source did not act as the agent of the center in gathering the information).

7. Originating agencies external to the CPIC are responsible for reviewing the quality and accuracy of the data provided to the center. The center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

8. The CPIC will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

H. Collation and Analysis

1. Information acquired or received by the CPIC or accessed for other sources will be analyzed only by qualified CPIC personnel who have successfully completed a background check and any applicable security clearance and have been selected, approved, and trained accordingly.

2. Information subject to collation and analysis is Information as defined and identified in Section E, Information of this policy.

3. Information acquired or received by the CPIC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:
   - Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the CPIC.
   - Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in criminal (including terrorist) activities.

The CPIC requires that all analytical products be reviewed by the Privacy Officer, or qualified designee as determined by the Commander of CPIC, to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

I. Merging Records

1. The set of identifying information sufficient to allow merging by the CPIC will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars;

social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

2. If the matching requirements are not fully met but there is an identified partial match, the information may be associated by the CPIC if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

J. Sharing and Disclosure

1. Credentialed, role-based access criteria will be used by the CPIC, as appropriate, to control:
   - **A.** The information to which a particular group or class of users can have access based on the group or class
   - **B.** The information a class of users can add, change, delete, or print.
   - **C.** To whom, individually, the information can be disclosed and under what circumstances

2. The CPIC adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

3. Access to or disclosure of records retained by the CPIC will be provided only to persons within the center or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information accessed will be kept by the CPIC.

4. Agencies external to the CPIC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

5. Records retained by the CPIC may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

6. Information gathered or collected and records retained by the CPIC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of five (4) years by the CPIC.

7. Information gathered or collected and records retained by the CPIC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the center for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

8. Information gathered or collected and records retained by the CPIC will not be:
   - Sold, published, exchanged, or disclosed for commercial purposes.
   - Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
   - Disseminated to persons not authorized to access or use the information.

9. There are several categories of records that will not be ordinarily not be provided to the public:
   - Pursuant to Illinois Freedom of Information Act, 5 ILCS 140 *et al.,* the following records will not be provided to the public:
     1. Information specifically prohibited from disclosure by federal or state law or rules and regulations implementing federal or state law.
     2. Private information, unless disclosure is required by another provision of this Act, a state or Federal law or a court order.
     3. Personnel information contained within public records, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, unless disclosure is consented to in writing by the individual subjects of the information.
     4. Records that relate to or affect the security of correctional institutions and detention facilities
     5. Preliminary drafts, notes, recommendations, memorandum and other records in which opinions are expressed, or policies or actions are formulated, except that a specific record or relevant portion of the record shall not be exempt when the record is publicly cited and identified by the head of the public body.
     6. Trade secrets and commercial or financial information from a person or business where trade secrets or commercial or financial information are furnished under a claim of proprietary, privileged or confidential, and that

disclosure would cause competitive harm to the person or business, and only insofar as the claim directly applies to the records requested.

7. Records relating to collective negotiating matters between public bodies and their employees or representatives, except that any final contract or agreement shall be subject to inspection and copying.
8. Records relating to a public body's adjudication of employee grievances or disciplinary cases; however, this exemption does not extend to the final outcome of cases in which discipline is imposed.
9. Information that would disclose or might lead to the disclosure of secret or confidential information, codes algorithms, programs, or private keys intended to be used to create electronic or digital signatures under the Electronic Commerce Security Act.
10. Vulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community, but not to the extent that disclosure could reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public. Information exempt under this item may include such things as details pertaining to the mobilization or deployment of personnel or equipment, to the operation of communication systems or protocols, or to tactical operations.
11. Records in the possession of any body created in the course of administrative enforcement proceedings, and any law enforcement or correctional agency for law enforcement purposes, but only to the extent that disclosure would:
    1. interfere with pending or actually and reasonably contemplated law enforcement proceedings conducted by any law enforcement or correctional agency that is the recipient of the request;
    2. interfere with active administrative enforcement proceedings conducted by the public body that is the recipient of the request;
    3. create a substantial likelihood that a person will be deprived of a fair trial or an impartial hearing;
    4. unavoidably disclose the identity of a confidential source, confidential information furnished only by the confidential source, or persons who file complaints with or provide information to administrative, investigative, law enforcement, or penal agencies; except that the identities of witnesses to traffic accidents, traffic accident reports, and rescue reports shall be provided by agencies of local government, except when disclosure would interfere with an active criminal investigation conducted by the agency that is the recipient of the request;
    5. disclose unique or specialized investigative techniques other than those generally used and known or disclose internal documents or correctional agencies related to detection, observation or investigation

of incidents of crime or misconduct, and disclosure would result in demonstrable harm to the agency or public body that is the recipient of the request;

6. endanger the life or physical safety of law enforcement personnel or any other person; or
7. obstruct an ongoing criminal investigation by the agency that is the recipient of the request.

- Information that meets the definition of "classified information" as the term is defined in the National Security Act, Public Law 235, Section 606.
- Information determined to be confidential under Section 4002 of the Technology Advancement and Development Act
- Information contained in local emergency plan submitted to a municipality in accordance with a local emergency plan ordinance that is adopted under Section 11-21.5-5 of the Illinois Municipal Code.
- Law enforcement officer identification information or driver information under Section 11-212 of the Illinois Vehicle Code.
- Information prohibited from being disclosed by the Personnel Records Review Act.
- Information prohibited from being disclosed by the Illinois School Student Records Act.
- Information that would violate an authorized nondisclosure agreement
- Information of personally identifiable health information pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and any other confidentiality law.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission.
- Other authorized basis for denial.

10. The CPIC will not confirm the existence or nonexistence of information to any person, or agency that would not be entitled to receive the information unless otherwise required by law.

K. Redress

K.1 Disclosure:

1. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in item 2, below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the CPIC. The individual may obtain a copy, if appropriate or required, of the information for the purpose of challenging the accuracy or completeness of the information. The CPIC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual. In Illinois, an individual's right to

access and review criminal history record information is codified under Title 20, Part 1210 of the Illinois Administrative Code

2. The existence, content, and source of the information will not be made available to an individual when **exempt from disclosure under 5 ILCS 140 and**:
   - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution.
   - Disclosure would endanger the health or safety of an individual, organization, or community.
   - The information is in a criminal intelligence information system subject to 28 CFR Part 23.
   - The information source does not reside with the center.
   - The CPIC or user agency did not originate or does not otherwise have a right to disclose the information.
   - Other authorized basis for denial (refer to Section J, Sharing and Disclosure).

   If the information does not originate with the CPIC, the requestor will be referred to the originating agency, if appropriate or required, or the CPIC will notify the source agency of the request and its determination that disclosure by the CPIC or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

K.2 Corrections

If an individual requests correction of information originating with the CPIC that has been disclosed, the CPIC's Privacy Officer or designee will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.

K.3 Appeals

The individual who has requested disclosure or to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the CPIC or the originating agency. The individual will also be informed of the procedure for appeal when the CPIC or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

K.4 Complaints

If an individual has a complaint with regard to the accuracy or completeness of any information and intelligence held by the CPIC that:

A. Is exempt from disclosure,

B. Has been or may be shared through the ISE,

i) Is held by the CPIC and
ii) Allegedly has resulted in demonstrable harm to the complainant,

The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the CPIC's Privacy Officer at the following e-mail address: cpicpo@chicagopolice.org or at that mailing address as found in Section N.1(2) of this policy. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the CPIC that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the CPIC Privacy Officer of all complaints and the resulting action taken in response to the complaint.

L. Security Safeguards

1. The CPIC's Senior Watch Officer (SWO) is designated and trained to serve as the CPIC's security officer.

2. The CPIC will operate in a secure facility that is protected from external intrusion. The CPIC will utilize secure internal and external safeguards against network intrusions. Access to the CPIC's databases from outside the facility will be allowed only over secure networks.

3. The CPIC will secure tips, leads and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

4. The CPIC will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by CPIC personnel authorized to take such actions.

5. Access to CPIC's information will be granted only to CPIC personnel whose positions and job duties require such access; who have successfully completed a background check and applicable security clearance; and who have been selected, approved, and trained accordingly.

6. Queries made to the CPIC's data applications will be logged into the data system identifying the user initiating the query.

7. The CPIC will utilize logs to maintain audit trails of requested and disseminated information (see Section N.2, Accountability, for more information on audit logs).

8. The CPIC will follow the data breach notification guidance set forth in the Illinois Personal Information Protection Act, 815 ILCS 530. The CPIC will:
    i. Notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person.
    ii. Any necessary notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the breach or any measures necessary to determine the scope of the breach and, if necessary, to restore the integrity of any information system affected by this release.

M. Information Retention and Destruction

1. The CPIC's Privacy Officer will ensure that all information is reviewed for record retention (validation or purge) in accordance with the Department's Form Retention Schedule and as provided by 28 CFR Part 23. For purposes of this Privacy Policy and for records retention and destruction purposes, suspicious activity reports will be treated as Chicago Police Department Information Reports which have a twelve (12) month retention.

2. When information has no further value or meets the CPIC's criteria for removal according to the Chicago Police Department's retention and destruction policy or according to the Illinois State Records Act, it will be purged, destroyed, and deleted or returned to the submitting agency.

3. The CPIC will delete information or return it to the originating agency once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency.

4. The CPIC's Privacy Officer will complete a Department To-From Subject report through the chain of command accompanied by a Record Destruction Report per Department policies and procedures and in accordance with the Department's Form Retention Schedule for notification of appropriate parties before information is deleted or returned in accordance with this policy or as otherwise agreed upon with the originating agency.

5. Notification of proposed destruction or return of records may or may not be provided to the submitting agency by the CPIC depending on the relevance of the information and any agreement with the originating agency.

N. Transparency, Accountability, and Enforcement

N.1 Information System Transparency

1. The CPIC will be open with the public in regard to information and intelligence collection policies and practices. The CPIC will make the CPIC's Privacy Policy available upon request and posted on the Center's Web page at www.chicagopolice.org.

2. The CPIC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The CPIC Privacy Officer can be contacted at:

   Chicago Police Department
   c/o CPIC Privacy Officer
   3510 S. Michigan, 4th Floor
   Chicago, IL 60653
   cpicpo@chicagopolice.org

N.2 Accountability

1. The audit log of queries made to the CPIC will identify the user initiating the query.

2. The CPIC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of five (5) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

3. The CPIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least semiannually and a record of the audits will be maintained by the CPIC Privacy Officer of the center.

4. CPIC's personnel or other authorized users shall report errors or suspected or confirmed violations of the CPIC's policies relating to protected information to the CPIC's Privacy Officer.

5. The CPIC will conduct periodic audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted by CPIC's Privacy Officer, or a designee as determined by the Superintendent of Police for the Chicago police Department. This person has the option of conducting a random audit at any time and without prior notice to the CPIC staff. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the CPIC's information and intelligence system(s).

6. The Department's Office of Compliance and/or CPIC's trained Privacy Officer will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy periodically and will make appropriate changes in response to

changes in applicable laws, technology, the purpose and use of the information systems and public expectations.

N.3 Enforcement

1. If center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Director of the CPIC will:
   - Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.
   - Suspend, demote, transfer, or terminate center personnel, as permitted by applicable Department personnel policies.
   - Apply administrative actions or sanctions as provided by Department General Order 93-03 entitled "Complaint and Disciplinary Procedures" and all addendum of General Order 93-03 in conjunction with the Rules and Regulations of the Chicago Police Department.
   - If the authorized user is from an agency external to the agency/center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy

2. The CPIC reserves the right to restrict the qualifications and number of personnel having access to CPIC information and to suspend or withhold service and deny access to participating agency or participating agency personnel violating the CPIC's Privacy Policy.

O. Training

1. The CPIC will require the following individuals to participate in training programs regarding implementation of and adherence to this privacy, civil rights, and civil liberties policy:
   - All assigned personnel of the CPIC.
   - Personnel providing information technology services to the CPIC.
   - Staff in other public agencies or private contractors providing services to the CPIC.
   - User who are not employed by the CPIC or a contractor.

2. The CPIC's privacy policy training program will cover:

   - Purposes of the privacy, civil rights, and civil liberties protection policy.
   - Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained or submitted by the CPIC to the shared space.

- How to implement the policy in the day-to-day work of the user, whether a paper or system user.
- The impact of improper activities associated with infractions within or through the agency.
- Mechanisms for reporting violations of the CPIC's privacy protection policies and procedures.
- The nature and possible penalties for policy violations, including possible transfer, dismissal, and criminal liability, and immunity, if any.

3. The CPIC will provide special training regarding the center's requirements and policies for collection, use and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

Appendix A—Terms and Definitions

The following is a list of primary terms and definitions used throughout this template. These terms may also be useful in drafting the definitions section of the agency's/center's privacy policy.

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Access Control—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Acquisition—The means by which an ISE participant obtains information through the exercise of its authorities, for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer either to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

Agency—The **CPIC** and all agencies that access, contribute, and share information in the **CPIC**'s justice information system.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—Authentication is the process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

Authorization—The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

Biometrics—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Center—Center refers to the Chicago Police Department's **Crime Prevention & Information Center or CPIC.**

Civil Liberties—Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Civil Rights—The term "civil rights" refers to governments' role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

Computer Security—Protection of information assets through the use of technology, processes, and training.

Confidentiality—Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

Credentials—Information that includes identification and proof of identification that is utilized by CPIC members to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates. Credentialed security access will be utilized to control:

- What information a class of users can have access to;
- What information a class of users can add, change, delete, or print; and
- To whom the information can be disclosed and under what circumstances.

Criminal Intelligence Information or Data—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information. The record is maintained per 28 CFR Part 23.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disk optical media.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and faxback systems. It does not include faxes, telephone calls, video

Fair Information Practices—The Fair Information Practices (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transporter Flows of Personal Data. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system. They are designed to:

1. Define agency purposes for information to help ensure agency uses of information are appropriate. ("Purpose Specification Principle")

2. Limit the collection of personal information to that required for the purposes intended. ("Collection Limitation Principle")

3. Ensure data accuracy. ("Data Quality Principle")

4. Ensure appropriate limits on agency use of personal information. ("Use Limitation Principle")

5. Maintain effective security over personal information. ("Security Safeguards Principle")

6. Promote a general policy of openness about agency practices and policies regarding personal information. ("Openness Principle")

7. Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency. ("Individual Participation Principle")

8. Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies. ("Accountability Principle")

Firewall—a security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

Fusion Center—A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

General Information or Data—Information that could include records, documents, or files pertaining to law enforcement operations, such as Computer Aided Dispatch (CAD) data, incident data, and management information. Information that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information could be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Homeland Security Information—As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

Information—Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, tips and leads data, suspicious activity reports, and criminal intelligence information.

Information Quality—Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy,

completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—A SAR that has been determined, pursuant to a two-part process established in the ISE_SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Intelligence-Led Policing (ILP)—A process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

Invasion of Privacy—Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

Law—As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information—For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Logs—Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals can access the system and the data.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases) and non-electronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Metadata—In its simplest form, metadata is information (data) about information, more specifically information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

Need to Know— As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

Nonrepudiation—A technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

Originating Agency—The agency or organizational entity that documents information or data, including source agencies that document SAR (and, when authorized, ISE-SAR) information that is collected by a fusion center.

Participating Agencies—An organization entity that is authorized to access or receive and use center information and/or intelligence databases and resources for lawful purposes through its authorized individual users.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in an activity or incident potentially related to terrorism.

Personally Identifiable Information—Personally identifiable information is one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious

affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).

- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).

- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).

- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons—Executive Order 12333 defines "United States persons" as a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the right to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy—A printed, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, disclosure, and access. The purpose of the privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and -implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection—A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information—For the nonintelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the

United States. For state, local, and tribal governments, these protections are derived from applicable state and tribal constitutions and state, local, and tribal laws, ordinances, and codes.

For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.

Public—Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the agency's/center's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

- Employees of the agency.
- People or entities—private or governmental—who assist the agency/center in the operation of the justice information system.
- Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

Public Access—Public access relates to what information can be seen by the public, that is, information whose availability is not subject to privacy interests or rights.

Record—Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Redress—internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

Repudiation—the ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Retention—Refer to Storage.

Right to Know—Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

Role-Based Access—A type of access that uses roles to determine rights and privileges. A role is a symbolic category of users that share the same security privilege.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Source Agency—Source agency refers to the agency or entity that originates SAR (and, when authorized, ISE-SAR) information.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the Information Technology industry than the second meaning.
2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Suspicious Activity—Observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Reports (SARs)—Reports that record the observation and documentation of a suspicious activity. Suspicious Activity Report (SAR) information offers a standardized means for feeding information repositories or data analysis tool. Any patterns identified during SAR review and analysis may be investigated in coordination with the reporting agency and, if applicable, the state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

Terrorism Information—Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism-Related Information—In accordance with the IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in the IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)) and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside the agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview reports (FIR). However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have an criminal offense attached or indicated, criminal history records, or Computer Aided Dispatch (CAD) data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without

further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on whether time and resources are available to determine its meaning.

Tips and leads information is maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

User—An individual representing a participating agency who is authorized to access or receive and use a center's information and intelligence databases and resources for lawful purposes.